JOURNAL OF ALGEBRA 150, 87–100 (1992)

Quadratic Residue Codes in Their Prime

HAROLD N. WARD

Department of Mathematics, University of Virginia, Charlottesville, Virginia 22903

Communicated by Walter Feit

Received September 25, 1990

INTRODUCTION

The algebraic route taken in [16] for the production of quadratic residue codes from the Weil representation of $SL(2, q)$, q a power of the odd prime p, required that p be invertible in the coefficient ring. But the spanning sets that result for the codes do not show this requirement. In fact, in Section 6 of the paper cited, a code over $GF(3)$ was read from these sets when $q=9$ for a construction of the Mathieu group M_{12}. The code is invariant under a monomial action of the larger group $\Gamma L(2, 9)$. This is a particular example of the general phenomenon to be described in the present paper.

The monomial action of $\Gamma L(2, q)$ on the projective line over the finite field $GF(q)$ that will be used extends that of $SL(2, q)$ for the quadratic residue codes. This action is given implicitly by some of the extra transformations found in [16]. $GF(q)$-codes invariant under this action or that for $GL(2, q)$ can be specified as doubly extended cyclic codes. The lattice of these codes turns out not to depend on p but only on the exponent m in $q=p^m$. It is isomorphic to the lattice of affine invariant binary codes of length 2^m; some of the details of the correspondence have parallels in [6]. The minimal code in the lattice, which we shall call the modular quadratic residue code, is the one obtained from the conventional spanning sets read into $GF(p)$.

Among these codes are those corresponding to binary Reed–Muller codes. When m is odd, one of these is a self-dual code in the middle of the lattice. For $m=3$ and $p=3$, it is even an extremal type III code of length 28 [13]. The dimensions of these codes do depend on p, and they can be calculated by recursive methods.

1. QUADRATIC RESIDUE CODES

The description of quadratic residue codes we shall use is based on [16] and follows from their construction as invariant subspaces for a monomial

0021-8693/92 $5.00

action of $SL(2, q)$ on the projective line over the finite field $GF(q)$. This approach incorporates the Gleason–Prange theorem in the definition and was first used by Gleason in producing the codes from induced representations. The exposition by van Lint and MacWilliams [10] provides an elementary derivation of the major features of the codes.

Let q be a power of the odd prime p and let $PL(q)$ be the projective line over $GF(q)$, consisting of $GF(q)$ itself and an extra element labeled ∞. The ambient space for quadratic residue codes has its standard basis labeled by the members of $PL(q)$: if $z \in PL(q)$, $[z]$ denotes the corresponding basis element. Usually the coefficients are taken from an appropriately chosen finite field. However, there are global codes with coefficients in a ring of characteristic 0; the entries of words can be read modulo prime ideals not dividing p to produce the codes over finite fields. This global approach was described by Assmus and Mattson [1] and used by Newhart to discuss minimum weights [14]. For our purposes, the ring D involved is obtained as follows: let χ be the quadratic character on $GF(q)$, given by $\chi(x) = 1$ if x is a nonzero square, -1 if x is a nonsquare, and 0 if $x = 0$. Put $\delta = \chi(-1)$ and let ρ be a square root of δq. Then D is the ring of integers in $\mathbb{Q}(\rho)$. This is $\mathbb{Z}$ if q is a square, and $\mathbb{Z}[(\sqrt{\delta\rho} + 1)/2]$ if not.

There are two global codes C_ε, $\varepsilon = \pm 1$. The spanning set for C_ε is labeled by the members of $PL(q)$,

$$e_\varepsilon(\infty) = \varepsilon\rho[\infty] + \sum [z],$$

$$e_\varepsilon(y) = \varepsilon\rho[y] + \delta[\infty] + \sum \chi(y - z)[z],$$

for $y \in GF(q)$; the sums are over $GF(q)$. If one wishes to reduce modulo a prime ideal divisor of 2, another spanning set is used [16, p. 166]. When the $\mathbb{Q}(\rho)$ spans are taken, $C_\varepsilon^\perp = C_{-\delta\varepsilon}$.

The group $GL(2, q)$ acts on $PL(q)$ by linear fractional transformations, $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ effecting the map $z \to (az + b)/(cz + d)$. The monomial action involved with quadratic residue codes is the representation induced from the character

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \to \chi(a)$$

of the stabilizer of ∞. It can be given in terms of the standard generators

$$R_a = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}, \qquad a \neq 0,$$

$$S_b = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

$$T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

The action formulas follow, with z standing for an arbitrary member of $PL(q)$ other than any singled out:

$$R_a\colon [\infty] \to \chi(a)[\infty], \qquad [z] \to [az],$$
$$S_b\colon [z] \to [z+b],$$
$$T\colon [\infty] \to [0] \to \delta[\infty], \qquad [z] \to \chi(z)[-1/z].$$

The action extends to one of $\Gamma L(2, q)$ by allowing the Frobenius map to act:

$$F\colon [z] \to [z^p].$$

The two codes are invariant under F, T, and the S_b and are switched or fixed by R_a according as $\chi(a) = -1$ or 1. The spanning elements transform in almost the way in which the standard basis elements do:

$$R_a e_\varepsilon(\infty) = e_{\chi(a)\varepsilon}(\infty), \qquad R_a e_\varepsilon(y) = \chi(a)\, e_{\chi(a)\varepsilon}(ay);$$
$$S_b e_\varepsilon(y) = e_\varepsilon(y+b);$$
$$Te_\varepsilon(\infty) = e_\varepsilon(0), \qquad Te_\varepsilon(0) = \delta e_\varepsilon(\infty), \qquad Te_\varepsilon(y) = \chi(y)\, e_\varepsilon(-1/y);$$
$$Fe_\varepsilon(y) = e_\varepsilon(y^p).$$

When the codes are read into finite fields of characteristics not p, with appropriate changes for characteristic 2, the results have dimensions $(q+1)/2$ and are acted upon in the same way as above by $\Gamma L(2, q)$. But if the spanning sets are read modulo a divisor of p, the entries involving ε become 0, and the result is a self-orthogonal code invariant under all of $\Gamma L(2, q)$. Its dimension is usually smaller than $(q+1)/2$, being equal only when $q = p$. It is a twice extended cyclic code. More generally, one can describe the invariant subspaces for $\Gamma L(2, q)$ in its monomial representation in characteristic p. Then this modular quadratic residue code turns out to be the smallest nontrivial one.

2. Twice Extended Cyclic Codes

In what follows a G-code will mean a G-invariant subspace of an ambient space on which the group G acts monomially. Let A be the ambient space over $GF(q)$ spanned by the $[z]$, $z \in PL(q)$, and let $\Gamma L(2, q)$ act on A by the formulas of Section 1. Then let A' be the once punctured space spanned by the $[z]$ with $z \neq \infty$, and A'' the twice punctured space

spanned by those with $z \neq \infty$ and $z \neq 0$. Think of R_a and S_b as acting on A', generating the so-called affine group Aff(q), and the R_a acting as a cyclic group of order $q-1$ on A''. For a code C in A, let C' and C'' be the corresponding punctured codes in A' and A'', obtained by deleting first the $[\infty]$ and then the $[0]$ coordinate. When C is a $GL(2, q)$-code, C' is an Aff(q)-code, and C'' is a cyclic code. In this case all three have the same dimension if $C \neq A$ itself. For a nonzero word in C supported on $[\infty]$ and $[0]$ alone would either have weight 1 or combine with an image under R_a, a not a square, to produce a nonzero word of weight 1. The transitivity of $GL(2, q)$ would then force $C = A$. Consequently, $C \to C''$ is injective and the three dimensions are the same. Since we shall wish to consider dual codes, let us designate A and 0 as trivial $GL(2, q)$-codes to be set aside for the moment.

Let $\sum'$ stand for a sum over $GF(q)$ and $\sum''$ for a sum over $GF(q) - \{0\}$.

PROPOSITION 2.1. *Let C be a nontrivial $GL(2, q)$-code. Then C and C' are extensions of the cyclic code C'': if $\sum'' \gamma_z[z] \in C''$, the corresponding words $\sum \gamma_z[z]$ and $\sum' \gamma_z[z]$ in C and C' satisfy the 0 and ∞ equations*:

$$\gamma_0 = -\sum'' \gamma_z, \tag{0}$$

$$\gamma_\infty = -\sum'' \chi(z)\,\gamma_z = -\sum' \chi(z)\,\gamma_z. \tag{∞}$$

Proof. Since $\dim C' = \dim C'' \leqslant \dim A'' < \dim A'$, C' is contained in the maximal Aff(q)-code, the subspace $\langle \sum'[z] \rangle^\perp$ (A' is the regular representation for the normal subgroup formed by the S_b). Thus $\sum' \gamma_z = 0$. Moreover, $T(\sum \gamma_z[z]) \in C$; that is,

$$\delta\gamma_0[\infty] + \gamma_\infty[0] + \sum'' \chi(z)\,\gamma_z[-1/z] \in C.$$

Equation (0) applied to this gives Eq. (∞).

The cyclic code C'' for a $GL(2, q)$-code is determined by a set of roots [11, Chap. 6]. Alternatively, one can give the exponents r for which $\sum'' \gamma_z z^r = 0$ for all the words $\sum'' \gamma_z[z]$ in C'', with these exponents construed as residue classes modulo $q-1$. Let E'' be the exponent set for C''; what properties must E'' have if C is nontrivial?

Suppose $c = \sum \gamma_z[z]$ and c is a typical member of C. By the transitivity of $GL(2, q)$, γ_0 is not always 0, and the 0 equation implies $0 \notin E''$. If $r \in E''$, evaluation of the equation for r at Tc implies that

$$\sum'' \chi(z)\,\gamma_z(-1/z)^r = 0.$$

Now $\chi(z) = z^{(q-1)/2}$; as that fraction occurs so often, let $j = (q-1)/2$. Then the equation becomes

$$\sum'' \gamma_z z^{j-r} = 0.$$

Thus $j - r \in E''$ also; in particular, $j \notin E''$.

Because the once extended code C' of C'' is affine invariant, the theorem of Kasami, Lin, and Peterson applies [9]: represent each exponent in the range $0 \leqslant r < q-1$ and write it base p. Let $s \leqslant_p r$ mean that each digit of s is at most the corresponding digit of r. Then if $r \in E''$ and $0 < s \leqslant_p r$, $s \in E''$ also.

The exponent set of $C''^{\perp}$ is the complement of $-E''$, which contains 0 and j. $C''^{\perp}$ thus extends to A with 0's at the $[\infty]$ and $[0]$ positions; so the exponent set $E''^{\perp}$ corresponding to $C^{\perp}$ is a subset of the complement of $-E''$. Since in general $\dim C'' = q - 1 - |E''|$, $E''^{\perp}$ is this complement with 0 and j removed. Now if $0 <_p r <_p j$, then $j <_p q-1-r <_p q-1$. As $q-1-r$ represents $-r$, $-r$ cannot be in the exponent set of a nontrivial $GL(2, q)$-code, otherwise j would be. So $-r \notin E''^{\perp}$, which means $r \in E''$. That is, E'' contains all the exponents in the interval $0 <_p r <_p j$ (and none with $j <_p r <_p q-1$). In particular, E'' is not empty if $q > 3$. Conversely, if E'' is not empty the conditions in the previous two paragraphs imply that all r with $0 <_p r <_p j$ are in E''.

We thus have necessary conditions on E'' for the code C as a twice extended cyclic code to be $GL(2, q)$ invariant; they are also sufficient:

PROPOSITION 2.2. *Let E'' be a set of exponents defining the cyclic code C'' in A''. Let C be the twice extended code in A given by the* 0 *and* ∞ *equations of Proposition* 2.1. *Then C is a nontrivial $GL(2, q)$-code if and only if*

(1) $0 \notin E''$,

(2) *$r \in E''$ implies $j - r \in E''$,*

(3) *if $r \in E''$ and $0 < s \leqslant_p r$, then $s \in E''$,*

(4) *if $q > 3$, E'' is nonempty.*

In addition, C is $\Gamma L(2, q)$ invariant exactly when

(5) *$r \in E''$ implies $pr \in E''$.*

Proof. Let such an E'' be given. Then C is nontrivial since $\dim C = q - 1 - |E''|$. Showing that C is $GL(2, q)$ invariant requires checking that when $c \in C$, $R_a c$, $S_b c$, and Tc all belong to C. The validity of the exponent membership equations for $R_a c$ is automatic from the cyclicity of C''; for $S_b c$ it follows from the Kasami, Lin, and Peterson theorem applied

for the once extended code C'. Condition (2) takes care of these equations for Tc. The affine invariance also covers the 0 equations for $R_a c$ and $S_b c$, and the ∞ equations for Tc hold by design ($T^2 = -\text{identity}$). The ∞ equation for $R_a c$ is routine, and only the ∞ equation for $S_b c$ has any subtlety:

$$\gamma_\infty = -\sum{}' \chi(z+b)\gamma_z.$$

With $\chi(z+b) = (z+b)^j$ again, and that factor expanded, it becomes

$$\gamma_\infty = -\sum_{k=0}^{j} \binom{j}{k} b^{j-k} \sum{}' z^k \gamma_z.$$

By the remarks leading to condition (4), the k for which the binomial coefficient is not 0, other than 0 and j, are all in E''. Thus the corresponding inner sums are 0. At $k = 0$, the sum is 0 by the 0 equation for c. The double sum has now become

$$\gamma_\infty = -\sum{}' z^j \gamma_z,$$

and that is the ∞ equation for c.

$\Gamma L(2, q)$ invariance is F invariance on top of $GL(2, q)$ invariance, and (5) is standard. Another way to say this is that C has a $GF(p)$ form.

It will prove helpful to include 0 and j artificially in the exponent sets:

DEFINITION 2.3. A quadratic set is a nonempty set E of exponents for which

(1) $r \in E$ and $0 \leqslant s \leqslant_p r$ implies $s \in E$,

(2) if $r \in E$, then $j - r \in E$,

(3) if $j <_p r$, then $r \notin E$.

By the discussion about the interval $0 < r <_p j$ preceding Proposition 2.2, these sets are the sets of that proposition augmented by 0 and j. If E corresponds to the code C, $C^\perp$ corresponds to the complement of $-E$ with 0 and j readjoined. This set will also be labeled $E^\perp$. The dimension of C is now $q + 1 - |E|$. A quadratic set for which $r \in E$ implies $pr \in E$ will be called cyclic.

3. The Binary Description of Quadratic Sets

If $q = p^m$, the exponents can be represented by numbers written base p with m digits. Let $p - 1 = g$ (suggesting a 9). Then 0 is represented by both $0 \cdots 0$ and $g \cdots g$. Formally this leads to $0 <_p r$ and $r <_p 0$, but that

ambiguity will not be a bother, as will become clear. In this arrangement $-r$ is represented by the "g's complement" of r, whose digits are g minus those of r. Arithmetic modulo $q-1$ can be effected by carrying or borrowing cyclically. For example, let $h=(p-1)/2$ ("half"), so that $j=h\cdots h$. Then with $r'=j-r$, r' is computed by doing the subtraction with cyclic borrowing when $r>j$. The exponent pr is obtained by cycling the digits of r to the left (whence the name "cyclic quadratic set").

PROPOSITION 3.1. *Let r and t be exponents for which $t\leqslant_p r\leqslant_p t'$. Then $t\leqslant_p r'\leqslant_p t'$ also. Given r, there is a unique minimal such t.*

Proof. When $r>_p j$, the minimal t will be j and t' will be 0 in the form $g\cdots g$. However, these exponents r do not appear in quadratic sets.

If x and x' are the digits in r and r' in a particular position, there are four possibilities for $x+x'$ depending on the carries in $r+r'$ to and from that position (in the cyclic scheme). They are as follows (the extremes are explained below):

Carry to	Carry from	$x+x'$	Extremes	
0	0	h	0	h
1	0	$h-1$	0	$h-1$
0	1	$p+h$	$h+1$	g
1	1	$g+h$	h	g

If a and a' are the corresponding digits in t and t', then $a\leqslant x\leqslant a'$, and consequently $a\leqslant a+(a'-x)\leqslant a'$. But $a+(a'-x)$ is the digit in $t+(t'-r)$ (in this parenthesizing there are no carries), and that is $t+t'-r=j-r=r'$. Thus $a+(a'-x)=x'$, and $a+a'=x+x'$. So the carry patterns in $r+r'$ and $t+t'$ are the same. The last columns list the minimum for a and the corresponding a'. These choices provide the needed extremes for t and t'. To find them in practice, lower x and raise x', maintaining the sum, until either x becomes 0 or x' becomes g.

An extremal pair t, t' will have digit sequences like the middle two rows here:

	0	0	$\cdots$	0	1	1	$\cdots$	1	0	
t:		0	$\cdots$	0	0	h	$\cdots$	h	$h+1$	0
t':	g	h	$\cdots$	h	$h-1$	g	$\cdots$	g	g	
	1	0	$\cdots$	0	0	1	$\cdots$	1	1	0

The top row indicates the carries from the right. For any exponent r, let $b(r)$ be the binary word of length m whose 1's are in the positions from

which there is a carry in $r+r'$. The bottom row shows the common word $b(t)=b(t')$. At an isolated 0 in $b(t)$ (with 1's on both sides), the t and t' entries are 0 and $h-1$, and at an isolated 1, they are $h+1$ and g. The exponents r with $b(r)=b(t)$ are those in the interval $t \leqslant_p r \leqslant_p t'$. Note that $b(r)=1\cdots1$ will not appear for qudratic sets.

PROPOSITION 3.2. *Let t_1, t_1' and t_2, t_2' be two extremal pairs of exponents, with corresponding binary words b_1 and b_2. Then $t_1 \leqslant_p t_2'$ if and only if $b_1 \leqslant_2 b_2$.*

Proof. If $b_1 \leqslant_2 b_2$, the nonzero entries of t_1 are under g's in t_2', and $t_1 \leqslant_p t_2'$. Conversely, if $t_1 \leqslant_p t_2'$, an $h+1$ in t_1 can only be under a g in t_2'. Although an h in t_1 could conceivably be under an h in t_2', to the right of the h in t_1 there would then be an h under an $h-1$ in t_2'. Again the nonzero entries in t_1 must be under g's in t_2', and $b_1 \leqslant_2 b_2$.

Now let E be a quadratic set. If $r \in E$, and t, t' form the extremal pair surrounding r, then t and t' are in E, since $t \leqslant_p r$ and $t'=j-t$. Along with them E contains all the exponents in the interval $t \leqslant_p s \leqslant_p t'$, including r'. This is just the set of exponents s for which $b(s)=b(r)$. Proposition 3.2 and these observations establish:

PROPOSITION 3.3. *Each quadratic set E corresponds to a nonempty set B of binary words of length m: $r \in E$ exactly when $b(r) \in B$. A nonempty set B of binary words comes from a quadratic set if and only if $1\cdots1 \notin B$ and B is closed; that is, if $b \in B$ and $a \leqslant_2 b$, then $a \in B$. E is cyclic exactly when B is cyclic, closed under cyclic shifts.*

If t, t' is an extremal pair, so is $-t', -t$, presented by g's complements. The corresponding binary word is the complement $1\cdots1+b(t)$ of $b(t)$. Consequently, if the binary set B corresponds to the quadratic set E, that corresponding to $E^\perp$ is the complement of the set of complements $1\cdots1+b$ of the members b of B. This will also be labeled $B^\perp$. The correspondence between nontrivial $GL(2, q)$-codes and closed binary sets is order reversing. Thus for completeness we let A correspond to the empty set and 0 to all of $GF(2)^m$. In summary:

THEOREM 3.4. *The lattice of $GL(2, q)$-codes is inversely isomorphic to the lattice of closed subsets of $GF(2)^m$. If code C corresponds to B, then $C^\perp$ corresponds to $B^\perp$. C has a $GF(p)$ form exactly when B is cyclic.*

These binary sets also correspond to the affine invariant binary codes of length 2^m.

4. The Minimal Code

All the nontrivial $GL(2, q)$-codes in A are contained in the code corresponding to the binary set $\{0\cdots0\}$, and they all contain its orthogonal, corresponding to the complement of $\{1\cdots1\}$. The exponents (including 0 and j) for the maximal code are those in the interval $0 \leqslant_p r \leqslant_p j$, $(h+1)^m$ of them. Its dimension is $(q+1)-(h+1)^m$ and that of the minimal code is $(h+1)^m$, that is, $((p+1)/2)^m$.

This minimal code is the one spanned by the images modulo a divisor of p of the elements $e_\varepsilon(z)$. The image words are

$$e(\infty) = \sum{}' [z],$$

$$e(y) = \delta[\infty] + \sum{}' \chi(y-z)[z].$$

They span a $\Gamma L(2, q)$-code by the transformation rules of Section 1. To see that it is the minimal code, determine the exponents. They are the r statisfying

$$\sum{}'' z^r = 0,$$

$$\sum{}'' \chi(y-z)\, z^r = 0,$$

for all y. The first equation holds for any $r \neq 0$. As usual, the second is

$$\sum{}'' (y-z)^j z^r = 0,$$

or

$$\sum_{k=0}^{j} y^{j-k}(-1)^k \binom{j}{k} \sum{}'' z^{k+r} = 0.$$

Since this must hold for all y, one needs

$$\binom{j}{k} \sum{}'' z^{k+r} = 0$$

for all k, $0 \leqslant k \leqslant j$. The binomial coefficient is nonzero for $k \leqslant_p j$, and the sum is 0 unless $k + r \equiv 0 \pmod{q-1}$. So r will be an exponent for the code unless $r \equiv -k \pmod{q-1}$ for some k with $0 \leqslant k \leqslant_p j$. But that exactly describes the exponent set for the minimal code.

Since the excluded exponents are numerically of the form $q-1-k$ with $0 \leqslant k \leqslant j$, the exponent set contains the interval from 1 to $j-1$. By the

BCH bound, the twice punctured code has minimum weight at least j, and the double transitivity of $GL(2, q)$ implies that the original code has minimum weight at least $j+2$. But

$$e(\infty)+e(0)=\delta[\infty]+[0]+2\sum[z],$$

the sum over the negatives of nonzero squares; this word has weight $j+2$. All together we have

THEOREM 4.1. *The minimal* $GL(2, q)$-code, *or modular quadratic residue code, is a* $GF(p)$-*code spanned by the elements* $\sum'[z]$ *and* $\delta[\infty]+\sum'\chi(y-z)[z]$, $y\in GF(q)$. *Its dimension is* $((p+1)/2)^m$ *and its minimum weight is* $(q+3)/2$.

When $m=1$, the code is a self-dual maximum distance separable code, equivalent to one discussed by Dür [7] and Blahut [2, p. 200].

Any linear transformation on A commuting with the monomial action of $GL(2, q)$ is determined by the image of $[\infty]$. The action of the S_b implies that $[\infty]\to\alpha[\infty]+\beta e(\infty)$ for some α and β, and then the R_a action requires $\beta=0$. Thus the commuting ring of A as a $GL(2, q)$-module is $GF(q)$ itself. In particular, if C is the modular quadratic residue code, C and $A/C^\perp$ afford inequivalent irreducible $GL(2, q)$ representations.

On the other hand, the map J: $[z]\to e[z]$ does commute with T and the S_b, and $JR_a=\chi(a)R_aJ$. Of course, $C=JA$, and as $\ker J$ is a $GL(2, q)$-module, it must be $C^\perp$. The commuting ring of $SL(2, q)$ is spanned by J and the identity. Thus $A/C^\perp$ and C are isomorphic as $SL(2, q)$-modules. Clifford's theorem implies that they are still irreducible; otherwise, they would reduce completely and the commuting ring would be larger than it is.

5. THE MIDDLE CODE

Another conspicuous code appears when m is odd, corresponding to the set B of binary words of weight less than $m/2$. $B^\perp=B$ and the code is self-dual. It has a $GF(p)$ form since B is cyclic.

For this code C, the square-root bound holds: if d is the minimum weight, $d\geqslant\sqrt{q-\frac{3}{4}}+\frac{3}{2}$ (unlike the traditional bound there is no dependence on δ; the proof follows from the multiple transitivity as in [16]). In fact, when $p\equiv 3 \pmod 4$ the improvement due to Heise and Kellerer [8] goes through: $d\geqslant(2/\sqrt{3})\sqrt{q-\frac{11}{12}}+\frac{4}{3}$.

One can also use the BCH bound as before. For any exponent r satisfying $0<r\leqslant 0\cdots 0h\cdots h$, with $(m+1)/2$ h's at the right, there are fewer

than $(m+1)/2$ carries in $r+r'=j$, so that $b(r)\in B$. But $0\cdots 0h\cdots(h+1)$ does involve $(m+1)/2$ carries. Thus there are $0\cdots 0h\cdots h$ consecutive exponents in the quadratic set for C; this number is $(p^{(m+1)/2}-1)/2$. Consequently, $d\geqslant(p^{(m+1)/2}+5)/2$. Roughly, $d\geqslant\sqrt{p}/2)\sqrt{q}$, while the Heise–Kellerer bound is approximately $d\geqslant(2/\sqrt{3})\sqrt{q}$. Only for $p=3$ is the latter better (it does not apply at $p=5$).

When $p=3$ and $m=3$, these results yield $d\geqslant 8$. Since the code is self-dual over $GF(3)$, its word weights are divisible by 3; so $d\geqslant 9$. One can also establish $d\geqslant 9$ by using the shifting technique of van Lint and Wilson [12]; the exponents are 1, 2, 3, 4, 6, 7, 9, 10, 11, 12, 18, 21. Since 9 is the upper bound for a (28, 14) type III self-dual code [13], this code is extremal (alternatively, the Griesmer bound rules out $d=12$). It appears to be new [3, p. 205], and its weight distribution is

$$A_0=1 \qquad A_{18}=2{,}159{,}976$$
$$A_9=2{,}184 \qquad A_{21}=1{,}555{,}632$$
$$A_{12}=78{,}624 \qquad A_{24}=216{,}216$$
$$A_{15}=768{,}096 \qquad A_{27}=2{,}240.$$

(The determination of the structure of minimum weight words in quadratic residue codes of length 27 leads naturally to this code [17]. It has also been constructed by Y. Cheng and R. Scharlau with different methods.)

As in Examples 7 and 8 of [10], the supports of the weight 9 words must form a single $GL(2, 27)$ orbit. Now the exponents for the code have 3-weight (base 3 digit sum) at most 3, as does j (= 13) itself. It follows that the code contains the extensions by 0 at $[\infty]$ of the words of the second order generalized Reed–Muller code [5]: the relevant computation is $2=3(3-1)-3-1$, where the 3's are, successively, m, p, and the 3-weight! Thus if H is any 2-dimensional flat in $GF(27)$ (as $GF(3)^3$), the code contains $c=\sum_{z\in H}[z]$. The words of weight 9 are the $GL(2, 27)$ images of $\pm c$.

6. Dimensions

Let b be a binary word of length m. The number of exponents r with $b(r)=b$ is the number for which $t\leqslant_p r\leqslant_p t'$, where t, t' is the extreme pair for b. By the display preceding Proposition 3.2, there are $h+1$ choices for a digit of r unless the digit is followed (cyclically) by a jump in b from 0 to 1 or 1 to 0. In that case there are only h choices. Thus if $\exp(b)$ is the number of such r and $j(b)$ is the number of jumps,

$$\exp(b)=(h+1)^{m-j(b)}h^{j(b)}.$$

If C is the $GL(2,q)$-code corresponding to a closed binary set B, its codimension is $\sum_{b\in B}\exp(b)$. This formula is correct even when $B=GF(2)^m$ and $C=0$. For $j(b)$ is always even, and to each jump pattern there correspond two words. Thus

$$\begin{aligned}\sum_{b\in GF(2)^m}\exp(b) &= 2\sum_k \binom{m}{2k}(h+1)^{m-2k}h^{2k}\\ &= (h+1+h)^m+(h+1-h)^m\\ &= p^m+1.\end{aligned}$$

For a binary set B, let $f_B=f_B(x)=\sum_{b\in B}x^{j(b)}$. The codimension of the corresponding code is $(h+1)^m f_B(h/(h+1))$. When p is large this is approximately $(h+1)^m|B|$.

As a special case, take for B the set of binary words of length m and weight $\leqslant w$. Let $C_{m,w}$ be the corresponding code. $C_{m,w}^{\perp}=C_{m,m-1-w}$, and the codes of Sections 4 and 5 are examples of these "Reed–Muller codes writ large," as one might call them. Let $f_{m,w}$ stand for f_B. Then $f_{m,w}=f_{m,m}$ for $w\geqslant m$, $f_{m,0}=1$ for $m\geqslant 1$; and, as above, $f_{m,m}=(1+x)^m+(1-x)^m$. The convention $f_{0,w}=2$ is compatible with this and the following recurrence relation:

PROPOSITION 6.1. *For m, $w\geqslant 0$,*

$$f_{m+2,w+1}=f_{m+1,w}+f_{m+1,w+1}+(x^2-1)f_{m,w}.$$

Proof. Suppose $0b$ is a word of length $m+2$ and weight $\leqslant w+1$, so that b has weight $\leqslant w+1$. Then $j(0b)=j(b)$ unless $b=1b'$ and b' either ends in 1 or is empty. In this case, $j(0b)=2+j(b)=2+j(b')$, with the empty word counted with no jumps. In the first case $x^{j(0b)}=x^{j(b)}$, and in the second

$$x^{j(0b)}=x^{j(b)}-x^{j(b')}+x^2x^{j(b')}=x^{j(b)}+(x^2-1)x^{j(b')}.$$

Similarly, if $1b$ has length $m+2$ and weight $\leqslant w+1$, then weight $(b)\leqslant w$ and again $j(1b)=j(b)$ unless $b=0b'$ with b' empty or ending in 0. The combined exceptions involve all words b' of length m and weight $\leqslant w$. Summing all possibilities gives the formula claimed.

In addition to the values for $f_{m,0}$ and $f_{0,w}$, one needs $f_{1,w}=2$ for $w\geqslant 1$ to start the recurrence.

These $f_{m,w}$ are cumulative sums of sectional polynomials $g_{m,w}$ defined by

$$g_{m,w}=\sum_{\substack{\text{weight}(b)=w\\ \text{length}(b)=m}}x^{j(b)}.$$

The $g_{m,w}$ satisfy the same recurrence as the $f_{m,w}$, but the initial values are $g_{0,0}=2$, $g_{m,0}=1$ for $m>0$, $g_{0,w}=0$ for $w>0$, $g_{1,1}=1$, and $g_{1,w}=0$ for $w>1$. In addition, $g_{m,m-w}=g_{m,w}$ for $w\leqslant m$.

The number of jumps in a binary word is the number of cyclic runs, and the number of words of length m and weight w having $2k$ runs is a classical quantity [4] equal to

$$\frac{m}{m-w}\binom{w-1}{w-k}\binom{m-w}{k}.$$

(0 if $m=w$). Thus

$$g_{m,w}=\sum_k \frac{m}{m-w}\binom{w-1}{w-k}\binom{m-w}{k}x^{2k}.$$

This can be expressed with a Jacobi polynomial [15, (4.3.2)]:

$$g_{m,w}(x)=\frac{m}{m-w}(1-x^2)^w P_w^{(-1,m-2w)}\left(\frac{1+x^2}{1-x^2}\right).$$

The transformations (4.1.3) and (4.22.1) of [15] change this to

$$g_{m,w}(x)=\frac{m}{m-w}P_w^{(-1,-m)}(1-2x^2).$$

TABLE I

	w						
m	0	1	2	3	4	5	6
1	2						
2	4	2					
3	8	6					
4	16	16	18				
5	32	40	50				
6	64	96	132	146			
7	128	224	336	406			
8	256	512	832	1,088	1,186		
9	512	1,152	2,016	2,832	3,330		
10	1,024	2,560	4,800	7,200	9,060	9,762	
11	2,048	5,632	11,264	17,952	24,024	27,654	
12	4,096	12,288	26,112	44,032	62,352	76,176	81,330

Then the three-term recurrence [15, (4.5.1)] yields, for a fixed m, the recurrence

$$\begin{aligned} w(m-w)(m+3-2w)\, g_{m,w} &= (m+2-w)\{(m+1-2w)(m+3-2w)\, x^2 \\ &\quad + 2(w-1)(m+1-w)\}\, g_{m,w-1} - (w-2) \\ &\quad \times (m+1-2w)(m+2-w)\, g_{m,w-2}. \end{aligned}$$

The starting values are $g_{m,0}=1$ and $g_{m,1}=mx^2$ for $m>1$.

Table I shows sectional dimensions $(h+1)^m g_{m,w}(h/(h+1))$ for $p=3$, when $h=1$ and $x=h/(h+1)=\frac{1}{2}$.

References

1. E. F. Assmus, Jr., and H. F. Mattson, Jr., New 5-designs, *J. Combin. Theory* 6 (1969), 122–151.
2. R. E. Blahut, "Theory and Practice of Error Control Codes," Addison–Wesley, Reading, MA, 1983.
3. J. H. Conway and N. J. A Sloane, "Sphere Packings, Lattices and Groups," Springer-Verlag, Berlin/Heidelberg/New York, 1988.
4. F. N. David and D. E. Barton, "Combinatorial Chance," Griffin, London, 1962.
5. P. Delsarte, J.-M. Goethals, and F. J. MacWilliams, On generalized Reed–Muller codes and their derivatives, *Inform. and Control* 16 (1974), 403–442.
6. S. R. Doty, The submodule structure of certain Weyl modules for groups of type A_n, *J. Algebra* 95 (1985), 373–383.
7. A. Dür, The automorphism groups of Reed–Solomon codes, *J. Combin. Theory Ser. A* 44 (1987), 69–82.
8. W. Heise and H. Kellerer, Über die Quadratwurzel-Schranke für Quadratische-Rest-Codes, *J. Geom.* 31 (1988), 96–99.
9. T. Kasami, S. Lin, and W. W. Peterson, Some results on cyclic codes which are invariant under the affine group and their applications, *Inform. and Control* 11 (1968), 475–496.
10. J. H. Van Lint and F. J. MacWilliams, Generalized quadratic residue codes, *IEEE Trans. Inform. Theory* IT-24 (1978), 730–737.
11. J. H. Van Lint, "Introduction to Coding Theory," Springer-Verlag, Berlin/Heidelberg/New York, 1982.
12. J. H. Van Lint and R. M. Wilson, On the minimum distance of cyclic codes, *IEEE Trans. Inform. Theory* IT-32 (1986), 23–40.
13. C. L. Mallows and N. J. A. Sloane, An upper bound for self-dual codes, *Inform. and Control* 22 (1973), 188–200.
14. D. Newhart, On minimum weight codewords in QR codes, *J. Combin. Theory Ser. A* 48 (1988), 104–119.
15. G. Szegö, "Orthogonal Polynomials," American Mathematical Society Colloquium Publications, Vol. 23, 4th ed., Amer. Math. Soc., Providence, RI, 1975.
16. H. N. Ward, Quadratic residue codes and symplectic groups, *J. Algebra* 29 (1974), 150–171.
17. H. N. Ward, Quadratic residue codes of length 27, *IEEE Trans. Inform. Theory* IT-36 (1990), 950–953.